GEO-BASED INTER-DOMAIN ROUTING (GIDR) PROTOCOL FOR MANETS

Biao Zhou[*], Abhishek Tiwari[+], Konglin Zhu[*], You Lu[$], Mario Gerla[*], Anurag Ganguli[+], Bao-hong Shen[+], David Krzysiak[#]
Corresponding Address: [+]UtopiaCompression Corporation, 11150 Olympic Boulevard, Suite # 680, Los Angeles, CA 90064, USA

Abstract

Inter-domain routing for MANETs (Mobile Ad Hoc Networks) draws increasing attention because of military and vehicular applications. The existing Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol for the Internet. But BGP is not applicable to MANETs because the BGP design is based on a static Internet which does not support dynamic discovery of members, and cannot scale to mobile, dynamic topology environments.

The proposed geo-based inter-domain routing (GIDR) protocol obtains efficient communications among MANETs and achieves scalability in large networks by using geo-routing packet forwarding scheme and clustering technique. The basic structure of GIDR is clusters in each domain. The distributed clustering algorithm elects within each domain a Cluster Head (CH). The cluster head in the subnet acts as local DNS for own cluster and also (redundantly) for neighbor clusters. The cluster head advertises to neighbors and the rest of the network its connectivity, members, and domain information. The advertising protocol plays the role of BG Protocol.

Geo-routing is the main packet forwarding scheme in GIDR. Assuming that all nodes are equipped with GPS, greedy forwarding is a straightforward routing scheme and can be easily standardized and implemented in all "coalition" nodes. Moreover, it is inherently scalable and is "address" independent (thus, it works across domain boundaries). If greedy forwarding fails, the packet is "directionally" forwarded to the "most promising" node along the advertised direction, i.e., direction forwarding. The experiments have shown that the proposed inter-domain routing has achieved scalability and robustness to mobility. The simulation results with Airborne Backbone Network, an important application domain in Military, as one of the domains are also presented in the paper.

I. INTRODUCTION

Nowadays, the inter-domain routing for MANETs (Mobile Ad Hoc Networks) draws more and more attention. The existing Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol for the Internet. But BGP is not applicable to MANETs because BGP design is based on a static Internet, and cannot scale to mobile, dynamic topology environments. The challenges in wireless, mobile inter-domain routing include dynamic network topology, intermittent connectivity, membership management, and routing protocol heterogeneity.

To meet the above challenges, the proposed geo-based inter-domain routing (GIDR) protocol tries to achieve scalability in the face of mobility by using geo-routing packet forwarding scheme and clustering technique. The basic structure of GIDR is clusters in each domain. The distributed clustering algorithm elects within each domain a Cluster Head (CH). The cluster head in the subnet acts as local DNS for own cluster and also (redundantly) for neighbor cluster. The cluster head advertises to neighbors and the rest of the network its connectivity, members, and domain information. The advertising protocol plays the role of BG Protocol.

Geo-routing is the main packet forwarding scheme in GIDR. Assuming that all nodes are equipped with GPS, greedy forwarding is a straightforward routing scheme, which forwards the packet to the neighbor yielding the most progress towards the destination. Greedy forwarding can be easily standardized and implemented in all "coalition" nodes. Moreover, it is inherently scalable and is "address" independent (thus, it works across domain boundaries).

The most delicate aspect of conventional Geo-Routing (and a damper to interoperability) is the circumvention of obstacles and "holes" using perimeter routing (a.k.a. face routing) methods. Perimeter routing greatly degrades performance. Moreover, no clear prevailing perimeter routing standard exists that will work well in all situations. This problem is bypassed by the use of directional forwarding in GIDR. If greedy forwarding fails, the GIDR packet is "directionally" forwarded to the "most promising" node along the advertised direction.

The proposed GIDR protocol has the following key characteristics and innovations: 1) Ability to handle frequent network topology changes by exploiting group affinity during cluster formation; 2) Dynamic discovery and dynamic split/merge; 3) Smaller routing table size and lower routing update frequency by the Geo-routing scheme (i.e., Greedy Forwarding + Direction Forwarding); 4) Member Digest implementation with Bloom Filter, enhancing GIDR scalability; 5) each MANET in GIDR preserves its legacy routing scheme, yet membership can evolve in time (split/expand/merge); and 6) Scalable to size and robust to mobility.

The rest of the paper is organized in the following way. The related work is briefly reviewed in section II. We describe the protocol design on GIDR in details in section III. Intensive performance evaluations are presented in section IV and we conclude in section VI.

II. RELATED WORK

We briefly review previous approaches related to inter-domain routing.

2.1 Border Gateway Protocol (BGP)

Inter-domain routing enables interoperations among heterogeneous domains that usually employ different routing protocols and policies. The Border Gateway Protocol (BGP) [3, 4] is the de facto inter-domain routing protocol for the Internet. BGP provides a standard mechanism for inter-domain routing among heterogeneous domains or autonomous systems (AS). The principle of BGP is to enable opaque interoperation, where each domain has the administrative control over its intra-domain routing protocol and inter-domain routing policy. In BGP, the routes to an internal destination within the same domain are determined by an intra-domain routing protocol, whereas the routes to an external destination are determined by the inter-domain routing policies among domains. BGP relies on a path vector protocol for exchanging inter-domain level reachability information. One of the advantages of the path vector protocol is that it makes it easy to detect a loop in a route. Also it makes it easy to specify domain administrator's preferences in the route selection thereby enabling a policy-based routing. Despite several reported inefficiencies, BGP has been operating non stop in the Internet for the past two decades. There is a vast body of literature on BGP and its properties, including scalability, control O/H and security. However, these results are not directly applicable to MANETs because

[*]Department of Computer Science, University of California, Los Angeles, CA 90095, USA
[$]Beijing University of Posts and Telecommunications, Beijing 100876, CHINA
[#]Air Force Research Lab, Rome Research Site/RIGC - Networking Technology, USA
Corresponding Email Addresses: [+]{abhishek, anurag, bao}@ utopiacompression.com

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Geo-Based Inter-Domain Routing (GIDR) Protocol for MANETS	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of California, Los Angeles,Department of Computer Science,Los Angeles,CA,90095**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
In IEEE Military Communications Conferences (MILCOM 2009), Boston, MA, October. 2009.

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**7**	

BGP design is based on a static Internet, and cannot survive in mobile, dynamic topology environments.

For example, BGP's capability to handle large numbers of routes makes it potentially valuable to large scale tactical networks. However, large scale causes slow convergence after routing changes. This is obviously not a significant issue in terrestrial networks, since links are generally very stable. But these BGP limitations are intensified by the MANET environment. Frequent network topology changes are possible due to the node movement in MANETs. Links can appear and disappear very quickly in this environment. Since BGP uses TCP for reliable control message exchange, it will be extremely vulnerable in such mobile environment. Likewise, BGP cannot support dynamic discovery of its members.

2.2 Other Previous Work (Besides BGP)

There are other proposals to enable inter-domain communications in the literature. Most of them focus on high level architectures and provide sketch of required components, e.g., the translation of naming spaces, protocol translation, BGP-style routing, and support for node mobility. Crowcroft et al. proposed Plutarch as architecture to translate address spaces and transport protocols among domains to support interoperation of heterogeneous networks [5]. TurfNet is another proposal for inter-domain networking without requiring global network addressing or a common network protocol [6].

2.2.1Mobile Ad hoc Inter-domain Networking (MAIN) Framework

The MAIN (Mobile Ad hoc Inter-domain Networking) framework recently proposed by [2, 1] assumes that each MANET functions as an autonomous system (AS) in the extended wireless Internet. It requires special gateway nodes in the networks. MAIN supports the policy-based routing, and relies on path vector protocol to support policy-based routing. In MAIN, the system of inter-connected MANETs is assumed to be traffic driven, i.e. reactive rather than proactive. Thus MAINS proposes a reactive path vector protocol. The proposed framework requires no surrender of the administrative control by each domain. Thus each domain can use its native intra-domain routing protocols without change, and specify inter-domain routing policies in the spirit of the policy-based routing as supported by BGP in the Internet.

But, there are several open issues that MAIN needs to handle: (a) partition and merge of domains; (b) membership announcement; (c) gateway function design; and (d) support for policy based routing. The first two points are due to node mobility and dynamic topology, and the latter two are general issues with inter-domain routing with autonomy of each domain.

2.2.2 Interconnecting Heterogeneous Routing solutions

Heterogeneous routing is a problem that must be faced when interconnecting MANETs. There have been proposals to take advantage of heterogeneous routing protocols to adapt to network dynamics and traffic characteristics. Hybrid routing protocols combine different style routing protocols and adaptively use them to improve the performance in a single domain. For example, SHARP [7] is an adaptive hybrid routing protocols that uses both proactive and reactive routing protocols to balance the tradeoff between the two and improve the performance. To achieve this goal, SHARP creates proactive routing zones around nodes with heavy traffic, and uses a reactive routing in other areas. Although hybrid routing combines different routing protocols, its main goal is to improve performance in a single zone via adaptation. On the contrary, this proposal studies the inter-networking of heterogeneous routing domains; it seeks solutions that are independent of the specific internal routing protocols.

Cluster-based networking [8] (such as LANMAR [11], ZRP [12]) is similar to inter-domain routing in that it is also concerned with the interaction among clusters of nodes at the network layer. The idea of cluster-based networking is to form self-organizing clusters and a routing backbone among cluster heads. In this way, cluster-based networks can achieve a scalable routing in a single domain. Although cluster-based routing has a structural similarity with inter-domain routing, there are fundamental differences. Inter-domain routing deals with multiple heterogeneous domains with autonomous control; the hierarchy of the network (i.e. domains) is given. On the other hand, in classic cluster-based routing the nodes are aggregated to form clusters. Normally Cluster-based networking is based on geographic proximity of the nodes. Thus it is more appropriate for a stationary rather than mobile network.

III. PROTOCOL DESIGN

3.1 Assumptions and Design Goals

In the proposed GIDR protocol, the following assumptions are made. Such assumptions are common when making inter domain routing [1][2].

- The node IDs are unique throughout the entire network. This is a valid assumption in that we can simply use the physical address (i.e., MAC address) of each node as its node ID, which guarantees a certain promise of uniqueness.
- The domain IDs are unique across the whole network. This only means originally the domain IDs are unique, and when domain splits we will use pseudo random generator to generate new domain IDs to retain this property.
- The communications between inter-domain gateways are bidirectional. This is also assumed in [1, 2].
- Domains are initially pre-assigned. Nodes in a domain normally running the same routing protocol. A domain may have multiple clusters depending on task assignments.
- Domain may be split due to node mobility or tasks changed, but nodes can merge and combine into new domains only if they are originally from the same domain. Since only nodes using the same intra-domain routing will be able to be combined into a same domain, this assumption is self-validate.

Besides the above assumptions, GIDR assumes that all nodes are equipped with GPS, which is common in military MANETs, such as Airborne Backbone networks.

The design of GIDR tries to meet the challenges in the inter-domain routing in MANETs. In the meantime, GIDR tries to bear the following properties:

- Scalability with network scale. Since the ad-hoc domain may have a large scale, GIDR should be scalable with respect to the node numbers.
- Robustness to mobility. Nodes in MANETs normally move frequently. The insensitivity to node motion is one of the goals of GIDR.
- Independent of intra-domain routing protocols. This means that the proposed GIDR protocol does not require the functionality of the underlying intra-domain routing. Because heterogeneous intra-domain routing protocols exist in different domains, this property of GIDR will allow it to adapt to different domains.

3.2 Basic Structure: Clusters

The basic structure of GIDR is clusters forming by the clustering techniques, which helps GIDR to obtain efficient communication among MANETs and to achieve scalability in large networks.

The proposed approach exploits the clustering by group affinity. In each domain, the distributed clustering algorithm discovers the set of "traveling companions" – these are the nodes that stick together as a group for some time or for some common tasks. It elects within each set a Cluster Head (CH) for each affinity group (Note that a cluster can have several cluster heads to obtain effective communications among domains). Affinity is defined in terms of some common characteristics, such as group motion or same tasks. The clusters (i.e., subnets) are defined a priori or evolve dynamically by the affinity of geography,

motion, or task. The cluster head in the subnet acts as local DNS for own cluster and also (redundantly) for neighbor clusters. The cluster head advertises to neighbors and the rest of the network its connectivity, members, and domain information (such as Autonomous System (AS) Id, etc). The advertising protocol plays the role of BG Protocol.

Note that the clustering algorithm requires periodic communications between nodes in the underlying pool nodes that are candidates to become members in the cluster. If the cluster uses a proactive routing algorithm, e.g. OLSR, the routing algorithm itself can be used for cluster creation and cluster-head election. In the case of on-demand routing like AODV and DSR, a separate periodic algorithm such as Distance Vector must be implemented to support the cluster functions and to propagate the cluster head advertisements across the cluster.

In GIDR, cluster heads (CH) function as gateways among domains and thus they can understand the messages or control packets from other domains. The control packet (i.e., the routing update packet) contains the topology table (including geo-locations of neighbors, etc.), the member list, and the AS Id of a cluster head. The information exchanged among cluster heads makes it possible to efficiently communicate with other CHs in different domains. They are also able to detect domain split and isolated nodes. The DSDV information exchange allows the proposed protocol to be independent of specific intra-domain routing protocols. On the other hand, non-CH nodes can't understand the control packets from other domains, but they will forward these control packets to their CHs.

Once the clusters are created and the cluster heads elected, the routing is a two level operation. In the proposed protocol, packets to remote nodes are routed via cluster-head advertised routes, and packets to local destinations are routed using the local routing algorithm. The cluster-head advertised route is discussed in details in next session 3.3.

3.3 Core Routing Components: Geo-DFR

Geo-DFR is of particular interest in multi-domain MANET scenarios, where a cluster head is elected in each domain and propagates advertisements to the other domains. GIDR uses Geo-DFR (Greedy Forwarding + Direction Forwarding) as its core components to route among domains. The packet travels from the source node's cluster head to the destination node's cluster head by using Geo-DFR [14]. From the latter it is delivered to the destination node via local routing protocol.

Geo-DFR is a geographical based routing scheme. The key idea of Geo-routing [13] is known that each node knows its geo-coordinates either from GPS or Galileo, and the source knows the destination geo-coordinates and stamps it in the packet. At each hop, the packet is forwarded to the neighbor closest to destination. Some forwarding schemes are used in Geo-routing, such as Greedy forwarding, Perimeter forwarding and Direction forwarding. In Geo-DFR, direction forwarding is designed to complement and even replace Perimeter forwarding in dead end recovery. A packet in Geo-DFR is first forwarded to the neighbor which yields the most progress towards the destination, i.e., greedy forwarding. If greedy forwarding fails, the packet is "directionally" forwarded to the "most promising" node along the advertised direction.

Figure 1 is the comparison between geo-routing (i.e., Greedy Forwarding here) and Geo-DFR. It also shows how direction forwarding in Geo-DFR helps packets to detour from a "hole", i.e., an obstacle. The upper part of Figure 1 illustrates the Geo-routing using greedy forwarding. When the node's routing run into a "hole", the greedy forwarding terminated, and the routing path fails because of the "hole". The lower part of Figure 1 shows the functionality of Geo-DFR. Each of nodes in Geo-DFR calculates the direction to the destination. If the greedy forwarding fails because of the "hole", the backup direction forwarding in Geo-DFR will be used to select the next hop for the further forwarding packets.

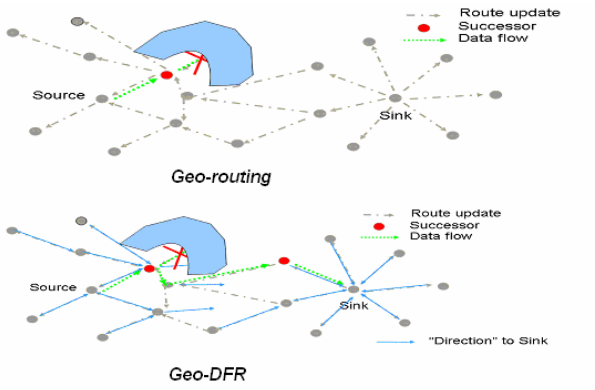

Figure 1: Comparison between Geo-routing and Geo-DFR.

The direction forwarding in Geo-DFR chooses the next hop based on the direction of each node to the destination which is calculated when the routing update received. Also, if multiple updates are received at the same time from different neighbors with same hop distance and sequence number, the direction will be calculated by the vector sum of directions. Figure 2 gives an example to illustrate the computing of the direction. Suppose Node A receives direction update packets from Node B and Node C, the direction to the destination is the vector sum of direction from Node A to Node B and the direction from Node A to Node C. It is marked with red color in Figure 2.

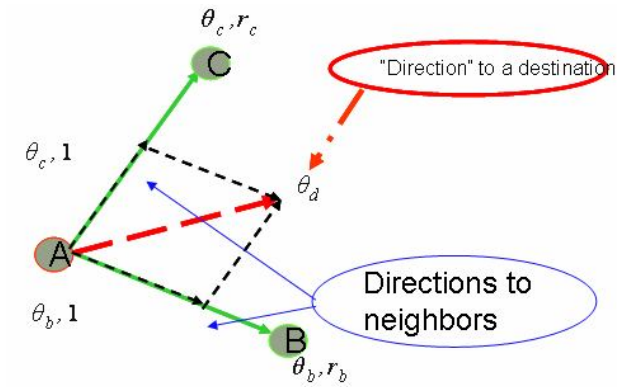

Figure 2: Computing the direction to the destination.

By using Geo-DFR, each node remembers the "direction" on the way to each cluster head in the same domain. The node knows which zone can be reachable from the cluster head. Among domains, cluster heads perform the Geo-DFR protocol to find an adoptive way to the destination as shown in Figure 3. Within the domain, an intra-domain routing protocol such as DSDV, AODV is used. The GIDR inter-domain routing protocol chooses the routing path which is marked by red lines from S to D in Figure 3.

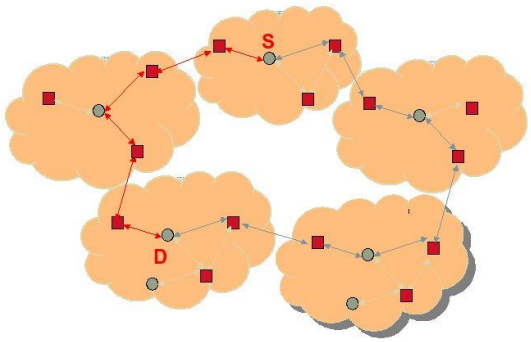

Figure 3: Scenario of GIDR.

3.4 Member Digest with Bloom Filter for Membership Management

The membership management in an inter-domain routing among MANETs is a challenge. The prefix based routing of BGP does not work since gateways are not able to aggregate domain members by suitable IP prefix.

Global gateways coordination and reassign node IDs so that each node has a unique prefix, which is not feasible. In the proposed GIDR protocol, the domain membership information is advertised in the form of membership digest. The advertised control packet broadcast by the CH node (i.e., gateway) contains the member digest of that domain.

Using a plain member list in the control packet by a CH is costly when the network becomes large. Bloom Filter [16] is the technique to map a member list to a bit vector, in which the membership verification operation can be carried out within *O(1)* operations instead of *O(m)* operations (*m* is the member count) required by the plain member list. When a Bloom Filter is used to represent the member list of a cluster, the size of the control packet advertised by CH is much smaller than the size of the conventional control packet which contains a plain member list. Thus the proposed GIDR protocol becomes more scalable by taking advantage of the Bloom Filter.

Figure 4 shows the construction of the Bloom Filter according to a plain member list. A bit vector of *m* bits is used to represent a set of *n* members $\{id_1, id_2, ..., id_n\}$. Originally all the bits in the Bloom Filter are set to '*0*'. By hashing each item using a hash function of $log_2(m)$ bits, the Bloom Filter will set the corresponding bit to '*1*'. To check the membership of the element *x*, it is sufficient to verify whether the bit corresponding to *h(x)* is set to '*1*'. The verification will cause false positive, i.e., an element not belonging to the set may be checked as a member. But Bloom Filter is free from false negatives, i.e., any element verified as a non-member shall not belong to the set. Many hash functions such as MD5 and SHA-1 are evenly distributed in the 'bit vector' domain, so the false positive probability can be decreased to a large extent.

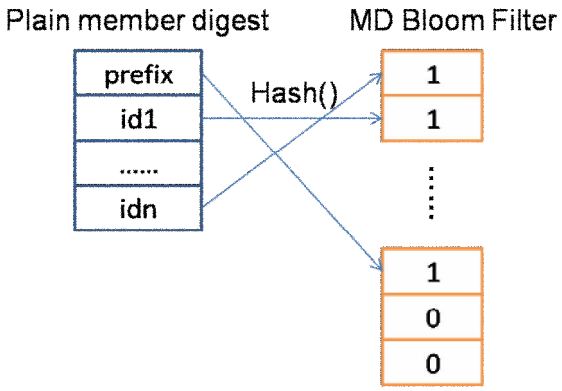

Figure 4: Using Bloom Filter to Compress the Member List.

3.5 Domain Split and Isolated Nodes

In the proposed GIDR protocol, Cluster heads (CHs) send periodic beacons to detect domain split. If one CH cannot hear any beacon from other CHs within the same domain, GIDR considers the domain as partitioned into disconnected components. A regular (non-CH) node within the domain will respond with an acknowledge message upon receiving the first beacon message from one of the CHs in the same domain. If regular nodes do not receive any beacon message within a timeout threshold, they will consider themselves as isolated nodes and trigger the new CH election algorithm to elect a new CH within these isolated nodes.

Either domain split or isolated nodes will trigger the birth of a new domain. A new AS ID needs to be generated. The member digest information and the timestamp of the new domain are fed into a pseudo random function, which will generate a new AS-ID for the new-born domain. The new AS-ID is guaranteed to be different from existing AS-IDs.

In the new-born domain, new cluster heads need to be elected. Each node in the domain triggers CH-election algorithm to elect a new CH. Since a CH with better connectivity is preferred, the CH-election algorithm will elevate the node with the most neighbors to CH rank. Using a neighbor discovery scheme, each node will know its number of neighbors, and broadcast this number to its neighbor. If it does not receive a neighbor count greater than its own neighbor count, it will elect itself as the CH. Note that the above CH-election algorithm is also applied to CH-election processes in existing domains.

With the birth of each new domain, we need to update the routing path in the routing tables of CHs in existing domains. Upon receiving the advertised update control packet from new-born domain, the CHs in existing domains will update their routing tables and membership information for the new-born domain. The GIDR protocol carefully adds domain information in order to prevent domain path loop. As long as the received domain ID is the same as the domain ID on the existing domain path, the advertised domain ID will be abandoned.

IV. Performance Evaluation

GIDR has been implemented in the QualNet net-work simulator 3.9.5 [9]. CBR sources generate network data traffic. The source-destination pairs are randomly selected. During a simulation run the number of connections is fixed, and thus the input traffic load is constant. The dimension of the network scenario is 1500m X 1500m. Different seeds are used in the simulations.

The mobility model is RPGM [10]. Each node in a domain has a common group motion component. In addition, each node has an individual intra-group motion component. In our simulation the group speed may vary under different scenarios, while the intra-group speed is fixed in the range of [0-5 m/s] and the pause time is 10 seconds.

The commonly used metrics of evaluating routing protocols for wireless ad hoc networks have been considered: 1) Packet Delivery Ratio: the ratio of the number of data packets delivered to the destination nodes over the number of data packets transmitted by the source nodes; and 2) Control Overhead: the total number of control packets for all delivered data packets during the whole simulation time.

In order to test the scalability of the proposed protocol and its robustness to mobility, its performances in various scenarios under different total node numbers and different CH percentages are evaluated. To show its independency of underlying intra-domain routings, we also tested GIDR with multiple domains running heterogeneous intra-domain routing protocols. The benefit of Bloom Filter applied in GIDR is also evaluated. To show the advantage of GIDR, the comparisons between GIDR and CIDR (Cluster-based Inter-Domain Routing), which is naturally developed based on the DSDV advertisement in the forming process of clusters within domains, are also evaluated. The simulation results with Airborne Backbone Network, an important application domain in Military, as one of naturally deployed domains are also presented in the paper.

The simulation parameters common to all experiments are as follows: PHY/MAC protocol is IEEE 802.11b, which has CSMA/CA with RTS/CTS, channel capacity of 2Mbps, and radio range of 375 meters. Total simulation time is 900 seconds.

4.1 Under Different Node Numbers and CH Percentages

To test the scalability of GIDR, the scenarios, which results are depicted in Figure 5 and 6, have different number of nodes per domain and different percentages of cluster heads. The percentage of cluster heads is the ratio of number of cluster heads over total node number in a domain. There are fixed two domains running different underlying routing protocols in these scenarios. The relationship between packet delivery ratio and different node number & CH percentage is shown in Figure 5. When the number of nodes in a domain increases, the

delivery ratio drops because of network congestion and rapid increase of control overhead (shown in Figure 6) in a dense network. When adding more cluster heads, the delivery ratio improves quickly since cluster heads function as the communicator between two domains and insufficient cluster heads may reduce the connectivity of the network and thus easily drop the packet.

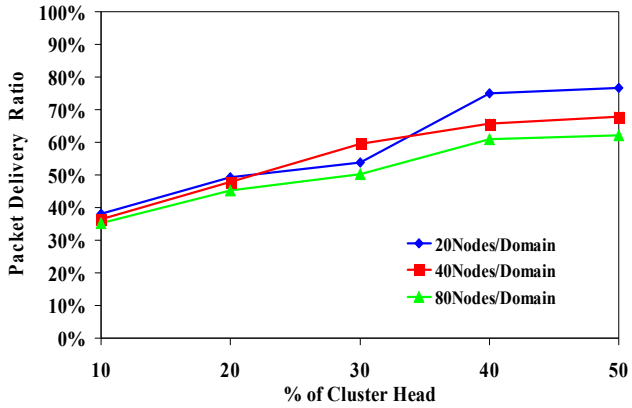

Figure 5: Packet Delivery Ratio vs. #Nodes/Domain & Percentage of CH.

Figure 6 shows the relationship between the control overhead and the number of nodes per domain & the percentage of cluster heads. Obviously, when more nodes exist in a domain, the routing control overhead of intra-domain increases a lot. The size of routing control packet to neighboring domain also becomes bigger because of more possible routing path entries in the domain. As we noticed in Figure 5 that the increasing cluster heads help the packet delivery, but it costs more control overhead. The reason is that each cluster head needs to handle the routing information and membership within the cluster and needs to broadcast such information to its neighboring cluster heads. More cluster heads thus produce more control overhead.

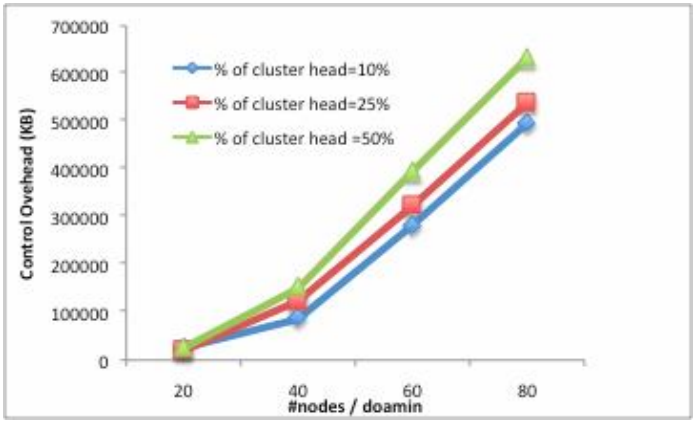

Figure 6: Control Overhead (OH) vs. #Nodes/Domain & Percentage of CH.

4.2 Under Multiple Domains

In order to show the GIDR independency of underlying routing protocols, the scenarios of Figure 7 and 8 have multiple domains, each of which runs different routing protocols, such as AODV, BELLMANFORD, FSRL, LAR1, RIP, or OSPF, etc. In these scenarios, the total node number in the whole network is fixed as 120. As shown in Figure 7, the packet delivery ratio drops when the number of domain increases. When the packet transfers across more domains, the possibility of packet loss increases since the packet needs to be routed by the "communicator" of cluster head and the number of cluster head in each domain is limited. As we can see from Figure 7, when more cluster heads are generated, the packet delivery ratio improves since more cluster heads function as communicators which reduce the packet loss.

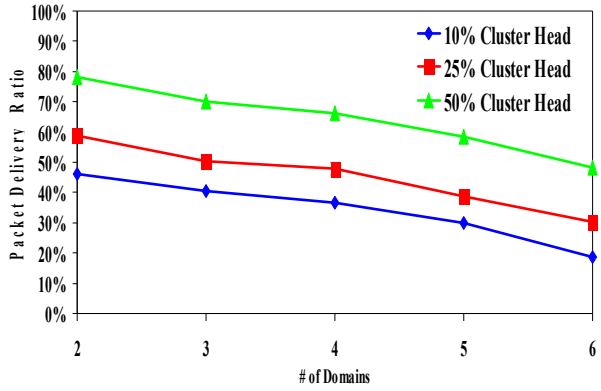

Figure 7: Packet Delivery Ratio vs. Number of Domains.

The relationship between the control overhead and number of domain is shown in Figure 8. When the number of domain increases, the routing overhead drops. In the scenarios of more domains, the intra-domain routing control overhead is greatly reduced because of smaller number of members per domain. The update frequency in intra-domain is normally much more frequent than that in inter-domain. Thus the total control overhead is less in the scenarios of more domains. The same trend is observed when the percentage of cluster head is increased. As we mentioned earlier, cluster head needs to generate and broadcast inter-domain control packet, and thus more control heads produce more control overhead.

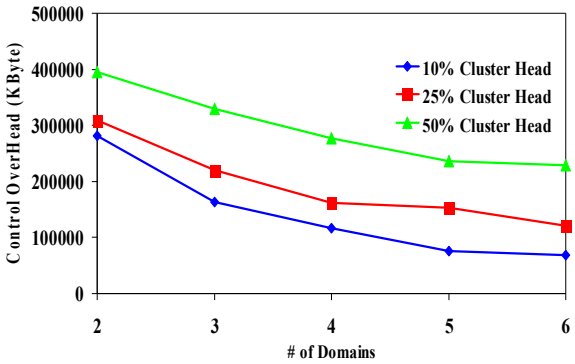

Figure 8: Control OverHead vs. Number of Domains.

4.3 Benefit of Bloom Filter

The effectiveness of bloom filter is based on member digest scheme. In our simulation, we use an 800-bit bloom filter as a hash table for the member digest. The bloom filter always compresses the member digest for each domain into this 800-bit hash table. Since each node address structure in QualNet is 32-bit, this bloom filter will introduce more overhead than a plain member digest when node number in each domain is less than 25 (e.g., 800/32). When the node number is greater than 25, bloom filter will help to decrease the control overhead in the proposed GIDR protocol. Figure 9 clearly indicates this phenomenon. In Figure 9, the X-Axis is the number of nodes in each domain, and the Y-Axis is the control overhead reduced by using a bloom filter compared to a plain member digest (i.e., the overhead of using plain member digest – the overhead of using bloom filter). When the node number in a domain is 20, this reduction is negative, meaning that the bloom filter introduces more overhead than plain member digest. When the node number in a domain is equal to or greater than 40, the bloom filter helps to alleviate the routing control overhead. Also we can see that when node number increases, the reduction by using bloom filter clearly increases.

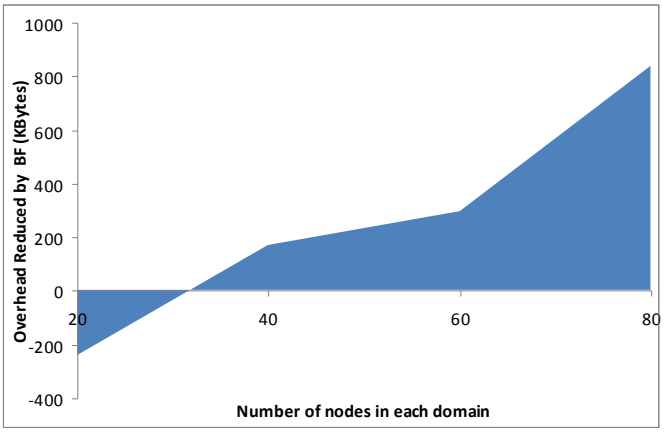

Figure 9: Effectiveness of bloom filter (BF) based member digest scheme.

4.4 Compare with Pure Cluster-based Inter-domain Routing (CIDR) using DSDV

As we discussed in session 3.2, CIDR can be naturally developed based on the DSDV advertisement in the forming process of clusters within domains. The major difference between GIDR and CIDR is that GIDR uses geo-based routing (i.e. Geo-DFR) among domains, but CIDR applies DSDV instead.

In order to illustrate the advantage of GIDR over CIDR, the scenarios of Figure 10 and 11 have two domains, 80 nodes per domain, and 20% cluster head among nodes with variety of velocity from 10 m/s to 50 m/s. The comparison results of delivery ratio between GIDR and CIDR is shown in Figure 10. We can see that there are huge delivery ratio differences between GIDR and CIDR, in which GIDR is almost 35% higher than CIDR protocol. The reason of better performance of GIDR over CIDR is the avoidance of stale routing table entries when using Geo-DFR in GIDR. The problem of stale routing table entries often happens in CIDR and drops packets when using DSDV in CIDR.

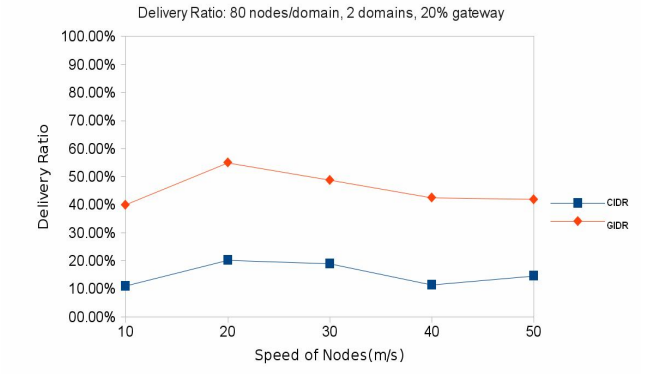

Figure 10: GIDR vs. CIDR (Delivery ratio comparison with variable of node speed).

Figure 11 shows the comparison results of control overhead between GIDR and CIDR. We can easily observe that GIDR generates much lower control overhead than that of CIDR. The reason is that GIDR protocol does not need to take so accurate routing information as CIDR requires. This will heavily reduce the size of update control packets and lower routing update frequency in GIDR, which reduce the control overhead of GIDR greatly. Based on the simulation results of Figure 10 and 11, GIDR shows a better performance than CIDR, no matter in the aspect of delivery ratio or control overhead.

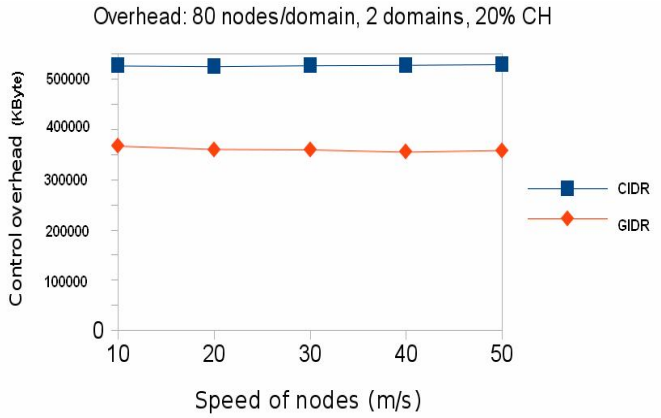

Figure 11: GIDR vs. CIDR (Control overhead comparison with variable of node speed).

4.5 Internetworking with Airborne Backbone Networks

GIDR can be naturally applied in the Airborne Network (AN) scenarios. Normally all of the nodes in airborne networks have GPS-equipped, thus it is able to know the geo-locations of neighboring nodes. The backbone nodes in the airborne networks naturally become the cluster heads in the GIDR protocol. The periodic communications among nodes in airborne networks provide the in-time routing information updates needed in GIDR. The Mobility aware paradigm (MARP [15]), which is a powerful and common used routing scheme inside one domain of airborne networks, may provide future geo-locations for nodes in airborne networks. This feature creates a more suitable environment to apply GIDR in airborne networks.

The simulation scenario of Airborne Backbone Network is illustrated in Figure 12. The Airborne Network backbone running MARP/MDP is composed of AWACs 1, Rivet Joint, JointStars, MC2A, GlobalHawk, Predator1, Predator2, U-2, AWACS. The nodes running BELLMANFORD are in the green shaded domain containing F-22, F-15 and F-22. The nodes running AODV are in the blue shaded domain containing F-22(9), F-15(10) and F-22(11). Each aircraft in the Airborne Network can be treated as backbone node and each of them can become a cluster head in GIDR. The backbone nodes in the AN can then communicate with cluster heads in two other MANETs under GIDR protocol.

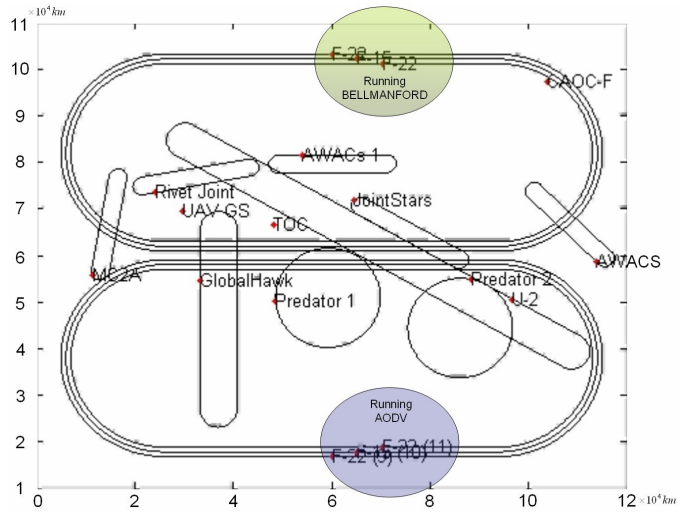

Figure 12: Simulation Scenario of Airborne Network.

The results of delivery ratio vs. velocity in Airborne Network scenarios are illustrated in Figure 13. The cluster head (CH) number of MANET domains in Figure 13 and 14 is fixed as 1. The curve with red nodes in Figure 13 represents the performance in the scenarios where

the number of cluster head in airborne domain is 1. The curve of blue nodes represents the scenarios where the cluster head number in airborne domain is 3. The pink one stands for the scenarios where the airborne domain has 5 cluster heads. Figure 13 shows that the delivery ratio becomes lower with the increasing of the velocity of the node. When nodes move faster, the radio links among nodes are frequently changed, which causes weaker node connectivity and thus reduces the packet delivery ratio. The relationship between the control overhead and node velocity is shown in Figure 14. The scenarios are the same as Figure 13. With the increase of node speed, the routing control overhead slightly increases because the faster node movement may produce more but not much more routing update packets.

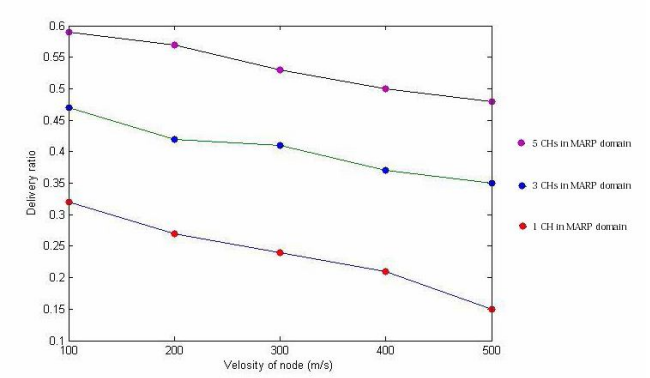

Figure 13: Delivery Ratio vs. Different Velocity (Airborne Network Scenario).

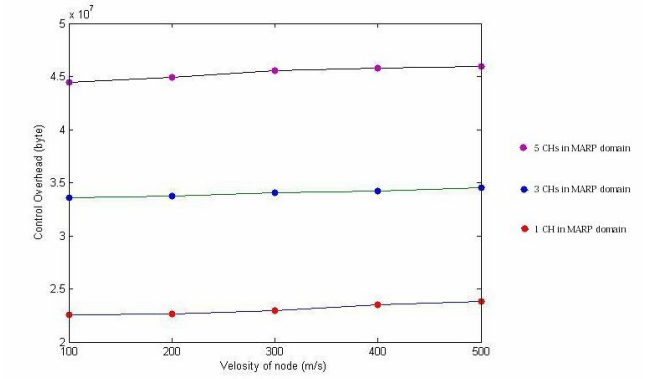

Figure 14: Control Overhead vs. Different Velocity (Airborne Network Scenario).

V. CONCLUSIONS

The proposed GIDR protocol achieves scalability in large networks by using Geo-DFR packet forwarding scheme and clustering technique. The basic structure of GIDR is clusters in each domain. The proposed approach exploits the clustering by group affinity. The elected cluster head in the subnet acts as local DNS for own cluster and also for neighbor clusters. The cluster head advertises to neighbors and the rest of the network its cluster information. The advertising protocol plays the role of BG Protocol.

GIDR applies Geo-DFR as its main packet forwarding scheme among domains. A packet in GIDR is first greedy forwarded to the neighbor which yields the most progress towards the destination cluster head. If greedy forwarding fails, the packet is "directionally" forwarded to the "most promising" node along the advertised direction.

The experiments have shown that the proposed inter-domain routing has achieved the scalability in large network, the robustness to mobility, and the independency of underlying intra-domain routing protocols. Compared to CIDR using DSDV, GIDR saves the routing table size, reduces the update frequency and avoids stale routing table entries, thus it produces higher delivery ratio and lower control overhead than CIDR. The simulation results with Airborne Backbone Network, an important application domain in Military, as one of the domains are also presented in the paper.

ACKNOWLEDGEMENT

The work presented in this paper is sponsored in part by the Air Force under the Small Business Innovation Research (SBIR) Phase II program, Air Force Research Laboratory (AFRL) at Rome Lab contract number FA8750-08-C-0127. This work was in collaboration with Professor Mario Gerla and his team under a subcontract to GPC. The authors would also like to thank MITRE Corporation, Bedford, MA for their guidance.

The concept of cluster head and geo-dfr routing is originally produced through participation in the International Technology Alliance sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defense, and by ARMY MURI.

REFERENCES

[1] Chi-Kin Chau, Jon Crowcroft, Kang-Won Lee, Starsky H.Y.Wong, "IDRM: Inter-Domain Routing Protocol for Mobile Ad Hoc Networks," Technical Report, Cambridge University.

[2] J. Crowcroft, et al, "Inter-domain Routing over Mobile Ad-hoc Networks", Hotmobile, 2008.

[3] Y. Rekhter and T. Li, "RFC 1771: a Border Gateway Protocol 4 (BGP-4)," March 1995.

[4] Susan Hares, Russ White, "BGP Dynamic AS Reconfiguration," IEEE Milcom 2007.

[5] J. Crowcroft, S. Hand, R. Mortier, T. Roscoe, and A. Warfield, "Plutarch: an argument for network pluralism," ACM Computer Communication Review, vol. 33, no. 4, pp. 258–266, 2003.

[6] S. Schmid, L. Eggert, M. Brunner, and J. Quittek, "Turfnet: An architecture for dynamically composable networks," in Proc. of 1st IFIP International Workshop on Autonomic Communication (WAC 2004), October 2004.

[7] V. Ramasubramanian, Z. J. Haas, and E. Sirer, "SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks," in Proc. ACM MOBIHOC, June 2003.

[8] Y. Chen, A. Liestman, and J. Liu, "Clustering algorithms for ad hoc wireless networks," in Proc. Ad Hoc and Sensor Networks '04, 2004.

[9] M. Takai, L. Bajaj, R. Ahuja, R. Bagrodia, M. Gerla. Glomosim: A Scalable Network Simulation Environment. Technical Report 990027; Univ. of California at Los Angeles, Computer Science Department, 1999.

[10] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang. A Group Mobility Model for Ad Hoc Wireless Networks. Proceedings of ACM/IEEE MSWiM'99; Seattle, WA, Aug. 1999.

[11] G. Pei, M. Gerla, X. Hong. LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility. Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing (MobiHoc 2000); Nov. 2000.

[12] Z.J. Haas and M.R. Pearlman. The Zone Routing Protocol (ZRP) for Ad Hoc Networks. Internet Draft, draft-ietf-manet-zone-zrp-02.txt, June 1999.

[13] X. Hong, K. Xu, and M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks", IEEE Network July/August 2002.

[14] Biao Zhou, Y. Lee and M. Gerla, ""Direction" Assisted Geographic Routing for Mobile Ad Hoc Networks". Milcom 2008.

[15] A. Tiwari, A. Ganguli, A. Sampath, D. Anderson, B. Shen, N. Krishnamurthi, J. Yadegar, M. Gerla, D. Krzysiak. Mobility Aware Routing for the Airborne Network Backbone. MILCOM 08; San Diego, Oct. 2008.

[16] A. Broder1, M. Mitzenmacher. Network Applications of Bloom Filters: A Survey. Internet Mathematics, vol. 1, no. 4, pp. 485–509, 2004.